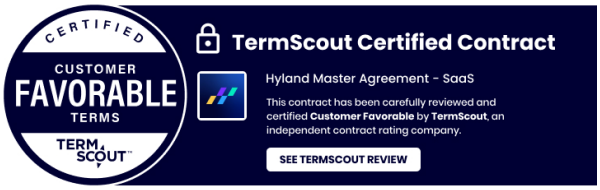

SAAS SECURITY ATTACHMENT

Introduction: Hyland maintains and manages a comprehensive written security program that covers the Hyland Cloud Service designed to protect: (a) the security and integrity of Customer Data; (b) against threats and hazards that may negatively impact Customer Data; and (c) against unauthorized access to Customer Data, which such program includes the following:

I. Risk Management.

a. Conducting an annual risk assessment designed to identify threats and vulnerabilities in the administrative, physical, legal, regulatory, and technical safeguards used to protect the Hyland Cloud Service.

b. Maintaining a documented risk remediation process to assign ownership of identified risks, establish remediation plans and timeframes, and provide for periodic monitoring of progress.

II. Information Security Program.

a. Maintaining a documented comprehensive Hyland Cloud Service information security program. This program will include policies and procedures based on industry standard practices, which may include ISO 27001/27002, or other equivalent standards.

b. Such information security program shall include, as applicable: (i) adequate physical and cyber security where Customer Data will be processed and/or stored; and (ii) reasonable precautions taken with respect to Hyland personnel employment.

c. These policies will be reviewed and updated by Hyland management annually.

III. Organization of Information Security. Assigning security responsibilities to appropriate Hyland individuals or groups to facilitate protection of the Hyland Cloud Service and associated assets.

IV. Human Resources Security.

a. Hyland employees undergo comprehensive screening during the hiring process. Background checks and reference validation will be performed to determine whether candidate qualifications are appropriate for the proposed position. Subject to any restrictions imposed by applicable law and based on jurisdiction, these background checks include criminal background checks, employment validation, and education verification as applicable.

b. Ensuring all Hyland employees are subject to confidentiality and non-disclosure commitments before access is provisioned to the Hyland Cloud Service or Customer Data.

c. Ensuring applicable Hyland employees receive security awareness training designed to provide such employees with information security knowledge to provide for the security, availability, and confidentiality of Customer Data.

d. Upon Hyland employee separation or change in roles, Hyland shall ensure any Hyland employee access to the Hyland Cloud Service is revoked in a timely manner and all applicable Hyland assets, both information and physical, are returned.

V. Asset Management.

a. Maintaining asset and information management policies and procedures. This includes ownership of assets, an inventory of assets, classification guidelines, and handling standards pertaining to Hyland assets.

b. Maintaining media handling procedures to ensure media containing Customer Data as part of the Hyland Cloud Service is encrypted and stored in a secure location subject to strict physical access controls.

c. When a Hyland Cloud Service storage device has reached the end of its useful life, procedures include a decommissioning process that is designed to prevent Customer Data from being exposed to unauthorized individuals using the techniques recommended by NIST to destroy data as part of the decommissioning process.

d. If a Hyland storage device is unable to be decommissioned using these procedures, the device will be virtually shredded, degaussed, purged/wiped, or physically destroyed in accordance with industry-standard practices.

VI. Access Controls.

a. Maintaining a logical access policy and corresponding procedures. The logical access procedures will define the request, approval and access provisioning process for Hyland personnel. The logical access process will restrict Hyland user (local and remote) access based on Hyland user job function (role/profile based, appropriate access) for applications and databases. Hyland user access recertification to determine access and privileges will be performed periodically. Procedures for onboarding and offboarding Hyland personnel users in a timely manner will be documented. Procedures for Hyland personnel user inactivity threshold leading to account suspension and removal threshold will be documented.

b. Limiting Hyland's access to Customer Data to its personnel who have a need to access Customer Data for performance under this Agreement. Hyland shall utilize the principle of "least privilege" and the concept of "minimum necessary" when determining the level of access for all Hyland users to Customer Data. Hyland shall require strong passwords subject to complexity requirements and periodic rotation and the use of multi-factor authentication.

c. Ensuring strict access controls are in place for Customer Data access by Hyland. Customer administrators control its user access, user permissions, and Customer Data retention to the extent such controls are available to Customer with respect to the Hyland Cloud Service.

VII. System Boundaries.

a. Hyland is not responsible for any system components that are not within the Hyland Cloud Platform, including network devices, network connectivity, workstations, servers, and software owned and operated by the Customer or other third parties. Hyland may provide support for these components at its reasonable discretion.

b. The processes executed within the Hyland Cloud Platform are limited to those that are executed by a Hyland employee (or Hyland authorized third party) or processes that are executed within Hyland's established system boundaries, in whole. This includes, but is not limited to, hardware installation, software installation, data replication, data security, and authentication processes.

c. Certain business processes may cross these boundaries, meaning one or more tasks are executed outside of Hyland's established system boundaries for the Hyland Cloud Platform, one or more tasks are executed by individuals who are not Hyland personnel (or authorized third-parties), or one or more tasks are executed based on written requests placed by Customer. In such event, Hyland will provide support for such processes to the extent they occur within Hyland's established system boundaries, but Hyland is not responsible for providing support for such processes to the extent they occur outside of such established system boundaries. At its reasonable discretion, Hyland may provide limited support for processes that occur outside such established system boundaries for the Hyland Cloud

Platform. Examples of business processes that cross these boundaries include, but are not limited to, Hyland Cloud Service configuration changes, processing that occurs within the Hyland Cloud Service, user authorization, and file transfers.

VIII. Encryption.

a. Customer Data shall only be uploaded to the Hyland Cloud Services in an encrypted format such as via SFTP, TLS/SSL, or other equivalent method.

b. Customer Data shall be encrypted at rest.

c. Where use of encryption functionality may be controlled or modified by Customer, in the event Customer elects to modify the use of or turn off any encryption functionality, Customer does so at its own risk.

IX. Physical and Environment Security.

a. The Hyland Cloud Platform uses data centers or third party service providers who have demonstrated compliance with one or more of the following standards (or a reasonable equivalent): International Organization for Standardization ("ISO") 27001 and/or American Institute of Certified Public Accountants ("AICPA") Service Organization Controls ("SOC") Reports for Services Organizations. These providers provide Internet connectivity, physical security, power, and environmental systems and other services for the Hyland Cloud Platform.

b. Hyland uses architecture and technologies designed to promote both security and high availability.

X. Operations Security.

a. Maintaining documented Hyland cloud operating procedures.

b. Maintaining change management controls to ensure changes to Hyland Cloud Service production systems made by Hyland are properly authorized and reviewed prior to implementation. Customer is responsible for testing all configuration changes, authentication changes and upgrades implemented by Customer or implemented by Hyland at the request of Customer prior to production use of the Hyland Cloud Service. In cases where the Customer relies upon Hyland to implement changes on its behalf, a written request describing the change must be submitted (e.g. an e-mail, or another method provided by Hyland) by Customer's designated Customer Security Administrators ("CSAs") or set forth in a Services Proposal. Hyland will make scheduled configuration changes that are expected to impact Customer access to their Hyland Cloud Service during a planned maintenance window. Hyland may make configuration changes that are not expected to impact Customer during normal business hours.

c. Monitoring usage and capacity levels within the Hyland Cloud Platform to adequately and proactively plan for future growth.

d. Utilizing virus and malware protection technologies, which are configured to meet common industry standards designed to protect the Customer Data and equipment located within the Hyland Cloud Platform from virus infections or similar malicious payloads.

e. Implementing disaster recovery and business continuity procedures. These will include replication of Customer Data to a secondary location.

f. Maintaining a system and security logging process to capture system logs deemed critical by Hyland. These logs shall be maintained for at least six months and reviewed on a periodic basis.

g. Maintaining system hardening requirements and configuration standards for components deployed within the Hyland Cloud Platform. Ensuring servers, operating systems, and supporting software used in the Hyland Cloud Platform receive all Critical and High security patches within a timely manner, but in no event more than 90 days after release, subject to the next sentence. In the event any such security patch would materially adversely affect the

Hyland Cloud Service, then Hyland will use reasonable efforts to implement compensating controls until a security patch is available that would not materially adversely affect the Hyland Cloud Service.

h. Conducting Hyland Cloud Platform vulnerability scans or analysis on at least a quarterly basis and remediate all critical and high vulnerabilities identified in accordance with its patch management procedures.

i. Conducting Hyland Cloud Platform penetration tests at least annually.

XI. Communications Security

a. Implementing Hyland Cloud Platform security controls to protect information resources within the Hyland Cloud Platform.

b. When supported, upon implementation and once annually thereafter, Customer may request Hyland limit access to Customer's Hyland Cloud Service to a list of pre-defined IP addresses at no additional cost.

XII. Supplier Relationships. Maintaining a Vendor Management Program for its critical vendors. This program will ensure critical vendors are evaluated on an annual basis.

XIII. Security Incident.

a. Employing incident response standards that are based upon applicable industry standards, such as ISO 27001:2013 and National Institute for Standards and Technology ("NIST"), to maintain the information security components of the Hyland Cloud Service environment.

b. Responses to these incidents follow the Hyland documented incident response sequence. This sequence includes the incident trigger phase, evaluation phase, escalation phase, response phase, recovery phase, de-escalation phase, and post-incident review phase.

c. If Hyland has determined Customer's Hyland Cloud Service has been negatively impacted by a security incident, Hyland will deliver a root cause analysis summary. Such notice will not be unreasonably delayed, but will occur after initial corrective actions have been taken to contain the security threat or stabilize the Hyland Cloud Service.

d. The root cause analysis will include the duration of the event, resolution, technical summary, outstanding issues, and follow-up, including steps Customer needs to take in order to prevent further issues. Hyland Cloud Service information including data elements that require additional confidentiality and security measures (including that of other customers impacted in the event) will not be publicly disclosed. If Customer needs additional details of an incident, a request to the Hyland GCS Support team must be submitted and handled on a case by case basis. The release of information process may require an on-site review to protect the confidentiality and security of the requested information.

e. Hyland will notify Customer of a Security Incident within 48 hours. A "Security Incident" means a determination by Hyland of an actual disclosure of unencrypted Customer Data to an unauthorized person or entity that compromises the security, confidentiality, or integrity of the Customer Data.

XIV. Information Security Aspects of Business Continuity Management.

a. Maintaining a business continuity and disaster recovery plan.

b. Reviewing and testing this plan annually.

XV. Aggregated Data.

a. Hyland owns all Customer and User registration and billing data collected and used by Hyland that is required for user set-up, use and billing for the Hyland Cloud Service ("Account Information") and all aggregated, anonymized and statistical data derived from the use and operation of the Hyland Cloud Service, including without limitation, the number of records in the Hyland Cloud Service, the number and types of transactions, configurations, and reports

processed as part of the Hyland Cloud Service and the performance results of the Hyland Cloud Service (the "Aggregated Data").

b. Hyland may utilize the Account Information and Aggregated Data for purposes of operating Hyland's business. For clarity, Account Information and Aggregated Data does not include Customer Data.

XVI. Security Inquiries.

a. Monitoring its compliance with its information security program. This includes periodic internal reviews. Results are shared with Hyland leadership and deviations tracked through to remediation.

b. Maintaining a periodic external audit program. Completed attestations, such as available SOC 2 reports, are provided to Customer upon written request.

c. Customer may conduct audits (which includes assessments, questionnaires, guided reviews or other requests to validate Hyland's security controls) (each a "Security Inquiry") of Hyland's operations that participate in the ongoing delivery and support of the Hyland Cloud Service purchased by Customer on an annual basis (but no more than once during any 12-month period); provided, that Customer provides Hyland with advance written notice of its desire to conduct such Security Inquiry and the proposed Security Inquiry does not overlap with, or otherwise cover the same or similar information as, or scope of: (1) any controls already provided for by an external audit or assessment already performed by Hyland, such as a SOC 2 report, ISO 27001 or other similar audit or assessment that is made available to Customer upon Customer's request; or (2) any content already provided by Hyland through its completed SIG, CAIQ or similar questionnaire that is made available to Customer upon request. For each Security Inquiry, (1) Hyland and Customer must mutually agree upon the timing, scope, and criteria of such Security Inquiry, which, subject to the foregoing, may include the completion of questionnaires supplied by Customer; (2) confidential and restricted documentation, such as Hyland internal policies, practices, and procedures, including any documentation requested by Customer that cannot be removed from Hyland's premises as a result of physical limitations or policy restrictions will not be provided externally or removed from Hyland's premises and such reviews must be conducted onsite at Hyland's corporate headquarters in Ohio or through a secure screenshare which may be arranged by Hyland to prohibit any type of copying or screen shots; (3) Customer understands and agrees that Hyland will not permit access to internal systems or devices used to host or support Hyland's offerings; (4) to the extent Customer desires to engage a third party to perform such Security Inquiry, Hyland must approve of such third party in writing in advance, Customer shall cause such third party to enter into a Non-Disclosure Agreement with Hyland and agree to abide by Hyland's security standards, and Customer shall manage the engagement with the third party, ensuring the third party understands the scope of the Security Inquiry as mutually agreed upon between Hyland and Customer and how Customer utilizes the Hyland Cloud Service; and (5) Customer shall pay Hyland fees (at Hyland's standard rates) for the Professional Services (including any out-of-pocket costs and expenses) that are required or requested of Hyland in connection with such Security Inquiry. Where necessary, Hyland will provide private and reasonable accommodation at Hyland's corporate headquarters in Ohio for data analysis and meetings. Upon reasonable advance written request, Hyland and Customer may mutually agree to make necessary employees or contractors available for interviews in person or on the phone during such Security Inquiry at Customer's cost and expense. Customer is prohibited, , and Customer shall prohibit each third party Security Inquiry from distributing or publishing the results of such Security Inquiry to any third party without Hyland's prior written approval. Notwithstanding anything to the contrary within this Agreement, nothing in this Agreement (including this section) will require Hyland or any of its affiliates to disclose information that is subject to attorney-client privilege.